Exhibit 4

Sign up   Sign in

Medium

Tornado.cash compliance

2 min read · Jun 3, 2020

Tornado Cash   Follow

Maintaining financial privacy is essential to preserving our financial freedom. However, it should not come at the cost of non-compliance.

We all remember the important event, of the blockchain history, that took place just a few months ago, when a user was blocked by one of the well-known centralized exchanges for trying to utilize a privacy solution. If you would like to read more about it, the full story can be found here.

That is why we decided to be ahead of the game and over the past few weeks implemented certain compliance-related tools including Tornado.cash Compliance Tool. If it ever becomes

Tornado.cash compliance. Maintaining financial privacy

https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370

Defense Exhibit

8793

S1 23 Cr. 403 (KPF)

necessary to show the origin of your assests you can provide cryptographically verified proof of transactional history using the Tornado.cash Note.

https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370

How does it work?

At the time of deposit, Tornado.cash generates a private Note that is used later to withdraw funds and can also be used to show their origin.

The only thing needed, in order to do so, is to enter your Tornado.cash Note into the Compliance Tool, generate a PDF report and forward it to the party of your choosing.

What makes this even more exciting, is that the other party can now verify the report directly from the Compliance Tool by using the Tornado.cash Note from the PDF report. This will in turn reduce, if not completely eliminate, the possibility of fraud or errors.

Why did we develop it?

We believe in honesty and transparency. Therefore, we advocate that every privacy oriented solution implement helpful tools such as this. Allowing users to protect their privacy should not come at the cost of violating the laws, rules or policies of centralized exchanges or other centralized entities.

Just remember, that Tornado.cash is a non-custodial privacy solution. Therefore, it is entirely up to you to either reveal your transactions to parties of your choice or keep them private forever. Keep in mind, that none of it is possible without the Tornado.cash Note and it is your responsibility to keep a record of it if you want to show the origin of funds later. However, if you loose it, we will not be able to help you since Tornado.cash doesn't keep any personal user data.

Restrictions

Just like Uniswap, we believe it's prudent to block IP addresses associated with US sanctioned countries on Tornado.cash domain. While we do not agree with the notion of censoring transactions, we would like to stay respectful of the US laws.

Going forward

Ultimately, Tornado.cash is a Community ran project. As such, we have open sourced our core protocol and our minified UI is available on github.

Once again, we would like to thank our helpful Community for their continuous contributions and support. If you have tips or suggestions on how we can make Tornado.cash better please let us know in our Telegram Channel.

Ethereum   Privacy   Blockchain   Zksnark   Compliance

Written by Tornado Cash

2.9K followers · 0 following

Non-custodial private transactions on Ethereum. tornado.cash